

Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

**Date: 22/07/2025 - 25/07/2025**





Contents

[Common Vulnerabilities and Exposures (CVEs) 3](#_Toc204328020)

[CISA/CERT-EU Alerts & Advisories 6](#_Toc204328021)

[News 7](#_Toc204328022)

[Breaches / Compromised / Hacked 8](#_Toc204328023)

[Vulnerabilities / Flaws / Zero-day 8](#_Toc204328024)

[Patches / Updates / Fixes 9](#_Toc204328025)

[Potential threats / Threat intelligence 9](#_Toc204328026)

[Guides / Tools 10](#_Toc204328027)

[References 11](#_Toc204328028)

[Annex – Websites with vendor specific vulnerabilities 12](#_Toc204328029)

# Common Vulnerabilities and Exposures (CVEs)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| URL ευπάθειας (NIST NVD) | CVSSv3 | Προϊόν/Υπηρεσία | Τύπος Ευπάθειας | Συσκευές/Εκδόσεις που επηρεάζονται | URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης |
| <https://nvd.nist.gov/vuln/detail/CVE-2025-7343> | **9,8** | SFT developed by Digiwin | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |  | https://www.digiwin.com/tw/news/3568.htmlhttps://www.twcert.org.tw/en/cp-139-10271-25ea9-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10270-83d95-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7916 | **9,8** | WinMatrix3 developed by Simopro Technology | Deserialization of Untrusted Data |  | https://www.twcert.org.tw/en/cp-139-10257-e88f3-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10256-14d55-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7918 | **9,8** | WinMatrix3 Web package developed by Simopro Technology | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |  | https://www.twcert.org.tw/en/cp-139-10264-6c4b7-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10259-b4b38-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7921 | **9,8** | Askey | Stack-based Buffer Overflow |  | https://www.twcert.org.tw/en/cp-139-10269-c9839-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10268-1583b-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2024-6107 | **9,6** | Canonical Ltd. | Improper Authentication |  | [ttps://bugs.launchpad.net/maas/+bug/2069094](https://bugs.launchpad.net/maas/%2Bbug/2069094%22%20%5Ct%20%22_blank) |
| https://nvd.nist.gov/vuln/detail/CVE-2025-47917 | **8,9** | Mbed TLS | Use After Free | Mbed TLS before 3.6.4 | https://github.com/Mbed-TLS/mbedtls-docs/blob/main/security-advisories/mbedtls-security-advisory-2025-06-7.mdhttps://mbed-tls.readthedocs.io/en/latest/tech-updates/security-advisories/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7344 | **8,8** | The EAI developed by Digiwin | Incorrect Use of Privileged APIs |  | https://www.digiwin.com/tw/news/3567.htmlhttps://www.twcert.org.tw/en/cp-139-10273-ce2ed-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10272-5b691-1.html |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7908 | **8,8** | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DI-8100 1.0 | https://github.com/buobo/bo-s-CVE/blob/main/DI-8100/wp.mdhttps://vuldb.com/?ctiid.317023https://vuldb.com/?id.317023https://vuldb.com/?submit.618582https://www.dlink.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7909 | **8,8** | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-513 1.0 | https://github.com/buobo/bo-s-CVE/blob/main/DIR-513/formLanSetupRouterSettings.mdhttps://vuldb.com/?ctiid.317024https://vuldb.com/?id.317024https://vuldb.com/?submit.618593https://www.dlink.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7910 | **8,8** | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DIR-513 1.10 | https://github.com/buobo/bo-s-CVE/blob/main/DIR-513/formSetWanNonLogin.mdhttps://vuldb.com/?ctiid.317025https://vuldb.com/?id.317025https://vuldb.com/?submit.618594https://www.dlink.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7911 | **8,8** | D-Link | Improper Restriction of Operations within the Bounds of a Memory Buffer | D-Link DI-8100 1.0 | https://github.com/buobo/bo-s-CVE/blob/main/DI-8100/upnp\_ctrl\_asp.mdhttps://vuldb.com/?ctiid.317026https://vuldb.com/?id.317026https://vuldb.com/?submit.618640https://vuldb.com/?submit.618641https://www.dlink.com/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7912 | **8,8** | TOTOLINK  | Improper Restriction of Operations within the Bounds of a Memory Buffer | TOTOLINK T6 4.1.5cu.748\_B20211015 | https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/6.mdhttps://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/6.md#pochttps://vuldb.com/?ctiid.317027https://vuldb.com/?id.317027https://vuldb.com/?submit.618655https://www.totolink.net/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7913 | **8,8** | TOTOLINK  | Improper Restriction of Operations within the Bounds of a Memory Buffer | TOTOLINK T6 4.1.5cu.748\_B20211015 | https://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/7.mdhttps://github.com/AnduinBrian/Public/blob/main/Totolink%20T6/Vuln/7.md#pochttps://vuldb.com/?ctiid.317028https://vuldb.com/?id.317028https://vuldb.com/?submit.618656https://www.totolink.net/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7914 | **8,8** | Tenda  | Improper Restriction of Operations within the Bounds of a Memory Buffer | Tenda AC6 15.03.06.50  | https://github.com/gaochen61/IoTVuln/blob/main/Tenda\_AC6\_V15.03.06.50/setparentcontrolinfo.mdhttps://vuldb.com/?ctiid.317029https://vuldb.com/?id.317029https://vuldb.com/?submit.618859https://www.tenda.com.cn/ |
| https://nvd.nist.gov/vuln/detail/CVE-2025-54317 | **8,4** | Logpoint  | Relative Path Traversal | Logpoint before 7.6.0 | <https://servicedesk.logpoint.com/hc/en-us/articles/28685507675549-Path-Traversal-in-Layout-Templates-Allows-Remote-Code-Execution> |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7915 | **7,3** | Chanjet CRM | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | Chanjet CRM 1.0 | https://github.com/qiantx/cve/blob/main/cve4.mdhttps://vuldb.com/?ctiid.317030https://vuldb.com/?id.317030https://vuldb.com/?submit.618873 |
| https://nvd.nist.gov/vuln/detail/CVE-2025-7917 | **7,2** | WinMatrix3 Web package developed by Simopro Technology | Unrestricted Upload of File with Dangerous Type |  | https://www.twcert.org.tw/en/cp-139-10263-5f2e7-2.htmlhttps://www.twcert.org.tw/tw/cp-132-10258-16bbf-1.html |

# CISA/CERT-EU Alerts & Advisories

|  |  |  |
| --- | --- | --- |
| Σύντομη περιγραφή / Τίτλος | Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες | URL |
| Joint Advisory Issued on Protecting Against Interlock Ransomware |  | <https://www.cisa.gov/news-events/alerts/2025/07/22/joint-advisory-issued-protecting-against-interlock-ransomware>  |
| CISA Releases Six Industrial Control Systems Advisories | * ICSA-25-205-01 [Mitsubishi Electric CNC Series](https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-01)
* ICSA-25-205-02 [Network Thermostat X-Series WiFi Thermostats](https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-02)
* ICSA-25-205-03 [Honeywell Experion PKS](https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03)
* ICSA-25-205-04 [LG Innotek Camera Model LNV5110R](https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-04)
* ICSMA-25-205-01 [Medtronic MyCareLink Patient Monitor](https://cisa.gov/news-events/ics-medical-advisories/icsma-25-205-01)
* ICSA-22-202-04 [ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update A)](https://www.cisa.gov/news-events/ics-advisories/icsa-22-202-04)
 | <https://www.cisa.gov/news-events/alerts/2025/07/24/cisa-releases-six-industrial-control-systems-advisories>  |
| LG Innotek Camera Model LNV5110R |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-04>  |
| Honeywell Experion PKS |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-03>  |
| Network Thermostat X-Series WiFi Thermostats |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-02>  |
| Medtronic MyCareLink Patient Monitor |  | <https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-205-01>  |
| Mitsubishi Electric CNC Series |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-205-01>  |
| CISA Adds Two Known Exploited Vulnerabilities to Catalog | * [CVE-2025-49704](https://www.cve.org/CVERecord?id=CVE-2025-49704" \o "CVE-2025-49704, ) Microsoft SharePoint Code Injection Vulnerability
* [CVE-2025-49706](https://www.cve.org/CVERecord?id=CVE-2025-49706" \o "CVE-2025-49706, ) Microsoft SharePoint Improper Authentication Vulnerability
 | <https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-adds-two-known-exploited-vulnerabilities-catalog>  |
| CISA Releases Nine Industrial Control Systems Advisories |  | <https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-releases-nine-industrial-control-systems-advisories>  |
| Schneider Electric EcoStruxture IT Data Center Expert |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-06>  |
| Schneider Electric System Monitor Application |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-05>  |
| Joint Advisory Issued on Protecting Against Interlock Ransomware |  | <https://www.cisa.gov/news-events/alerts/2025/07/22/joint-advisory-issued-protecting-against-interlock-ransomware>  |
| Schneider Electric EcoStruxure |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-03>  |
| Lantronix Provisioning Manager |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-02>  |
| DuraComm DP-10iN-100-MU |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-01>  |
| Schneider Electric EcoStruxure Power Operation |  | <https://www.cisa.gov/news-events/ics-advisories/icsa-25-203-04>  |
| CISA Adds Four Known Exploited Vulnerabilities to Catalog |  | <https://www.cisa.gov/news-events/alerts/2025/07/22/cisa-adds-four-known-exploited-vulnerabilities-catalog>  |
| Joint Advisory Issued on Protecting Against Interlock Ransomware |  | <https://www.cisa.gov/news-events/alerts/2025/07/22/joint-advisory-issued-protecting-against-interlock-ransomware>  |
| #StopRansomware: Interlock |  | <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a>  |

# News

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| SharePoint 0-day Vulnerability Exploited in Wild by All Sorts of Hacker Groups | <https://cybersecuritynews.com/sharepoint-0-day-vulnerability-exploited/>  |
| Metasploit Module Released For Actively Exploited SharePoint 0-Day Vulnerabilities | <https://cybersecuritynews.com/metasploit-module-for-sharepoint-0-day/>  |
| AWS Client VPN for Windows Vulnerability Let Attackers Escalate Privileges | <https://cybersecuritynews.com/aws-client-vpn-for-windows-vulnerability/>  |
| CISA warns of Google Chromium 0-Day Input Validation Vulnerability Exploited in Attacks | <https://cybersecuritynews.com/cisa-google-chromium-0-day/>  |
| UNC3944 Attacking VMware vSphere and Enabling SSH on ESXi Hosts to Reset ‘root’ Passwords | <https://cybersecuritynews.com/unc3944-attacking-vmware-vsphere/>  |
| Key Administrator of World’s Most Popular XSS Dark Web Cybercrime Platform Arrested | <https://cybersecuritynews.com/key-admin-russian-cybercrime-forum/>  |
| How Businesses Prevent Credential Theft with Early Phishing Detection | <https://cybersecuritynews.com/how-businesses-prevent-credential-theft-with-early-phishing-detection/>  |
| Windows 11 Gets New AI-Powered Features – Discover What’s New | <https://cybersecuritynews.com/windows-11-ai-powered-features/>  |
| Brave Browser Blocks Microsoft Recall by Default Due to Privacy Concerns | <https://cybersecuritynews.com/brave-browser-blocks-microsoft-recall/>  |
| Critical Vulnerability in JavaScript Library Exposes Millions of Apps to Code Execution Attacks | <https://cybersecuritynews.com/javascript-library-vulnerability/>  |
| Ransomware Gangs Leveraging RMM Tools to Attack Organizations and Exfiltrate Data | <https://cybersecuritynews.com/ransomware-gangs-leveraging-rmm-tools/>  |
| Hackers Injected Malicious Firefox Browser Packages to Arch Linux User Repository | <https://cybersecuritynews.com/malicious-aur-packages/>  |
| Windows 11 Gets New Black Screen of Death With Auto Recovery Tool | <https://cybersecuritynews.com/black-screen-of-death/>  |
| CISA Warns of Microsoft SharePoint Code Injection and Authentication Vulnerability Exploited in Wild | <https://cybersecuritynews.com/cisa-sharepoint-code-injection/>  |
| Kali Linux Unveils Two New Tools to Boost Wi-Fi Performance for Raspberry Pi Users | <https://cybersecuritynews.com/kali-linux-new-wi-fi-packages/>  |
| Chinese Hackers Actively Exploiting SharePoint Servers 0-Day Flaw in the Wild | <https://cybersecuritynews.com/chinese-hackers-exploiting-sharepoint-servers-0-day/>  |
| CISA Warns of Interlock Ransomware With Double Extortion Tactics Attacking Windows and Linux Systems | <https://cybersecuritynews.com/interlock-ransomware-attack/>  |
| Threat Actors Allegedly Selling macOS 0-day LPE Exploit on Hacker Forums | <https://cybersecuritynews.com/macos-0-day-lpe-exploit/>  |
| UK Confirms Ban of Ransomware Payments to Public and Critical National Infrastructure Sectors | <https://cybersecuritynews.com/uk-bans-ransomware-payments/>  |
| ETQ Reliance RCE Vulnerability Enables Full SYSTEM Access Just by Typing a Single Space | <https://cybersecuritynews.com/etq-reliance-rce-vulnerability/>  |
| UK Sanctions Russian APT 28 Hackers for Attacking Microsoft Cloud Service Login Details | <https://cybersecuritynews.com/uk-sanctions-russian-apt-28-hackers/>  |
| New DCHSpy Android Malware Steals WhatsApp Data, Call Logs, Record Audio and Take Photos | <https://cybersecuritynews.com/new-dchspy-android-malware/>  |

## Breaches / Compromised / Hacked

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| Dior, a Louis Vuitton Brand, Alerts Customers Following Cyber Attack | <https://cybersecuritynews.com/louis-vuitton-cyber-attack/>  |

## Vulnerabilities / Flaws / Zero-day

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| TP-Link Network Video Recorder Vulnerability Let Attackers Execute Arbitrary Commands | <https://cybersecuritynews.com/tp-link-network-video-recorder-vulnerability/>  |
| GitLab Security Update – Patch for Multiple Vulnerabilities in Community and Enterprise Edition | <https://cybersecuritynews.com/gitlab-security-update-patch-for-multiple-vulnerabilities/>  |
| Firefox 141 Released With Fix for Multiple Vulnerabilities – Update Now | <https://cybersecuritynews.com/firefox-141-released-fix-for-vulnerabilities/>  |
| US Nuclear Weapons Agency Breached by Hackers Using Microsoft SharePoint 0-Day Vulnerability | <https://cybersecuritynews.com/us-nuclear-weapons-agency-breached/>  |
| CISA Warns of Chinese Hackers Exploiting SharePoint 0-Day Flaws in Active Exploitation | <https://cybersecuritynews.com/cisa-chinese-hackers-sharepoint-0-day/>  |
| Chrome High-Severity Vulnerabilities Allow Attackers to Execute Arbitrary Code | <https://cybersecuritynews.com/chrome-type-confusion-attacks/>  |
| Apache Jena Vulnerability Leads to Arbitrary File Access or Manipulation | <https://cybersecuritynews.com/apache-jena-vulnerability/>  |
| New Scanner Released to Detect SharePoint Servers Vulnerable to 0-Day Attack | <https://cybersecuritynews.com/scanner-released-sharepoint-0-day/>  |
| Critical Sophos Firewall Vulnerabilities Enables pre-auth Remote Code Execution | <https://cybersecuritynews.com/sophos-firewall-vulnerabilities-rce/>  |
| Cisco Warns of Identity Services Engine RCE Vulnerability Exploited in the Wild | <https://cybersecuritynews.com/cisco-ise-rce-vulnerability-exploited-in-wild/>  |
| ExpressVPN Windows Client Vulnerability Exposes Users Real IP Addresses With RDP Connection | <https://cybersecuritynews.com/expressvpn-windows-client-vulnerability/>  |
| Microsoft Releases Mitigations and Threat Hunting Queries for SharePoint Zero-Day | <https://cybersecuritynews.com/sharepoint-zero-day-patch/>  |

## Patches / Updates / Fixes

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| Wireshark 4.4.8 Released With Bug Fixes and Updated Protocol Support | <https://cybersecuritynews.com/wireshark-4-4-8-released/>  |

## Potential threats / Threat intelligence

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
| Rise in Phishing Activity Using Spoofed SharePoint Domains With Sneaky2FA Techniques | <https://cybersecuritynews.com/rise-in-phishing-activity-using-spoofed-sharepoint-domains/>  |
| Elephant APT Group Attacking Defense Industry Leveraging VLC Player, and Encrypted Shellcode | <https://cybersecuritynews.com/elephant-apt-group-attacking-defense-industry/>  |
| BlackSuit Ransomware’s Data Leak and Negotiation Portal Seized | <https://cybersecuritynews.com/blacksuit-ransomware-portal-seized/>  |
| First Known LLM-Powered Malware From APT28 Hackers Integrates AI Capabilities into Attack Methodology | <https://cybersecuritynews.com/llm-powered-malware-from-apt28-hackers-integrates-ai-capabilities/>  |
| NoName057(16)’s Hackers Attacked 3,700 Unique Devices Over Last Thirteen Months | <https://cybersecuritynews.com/noname05716s-hackers-attacked-3700-unique-devices/>  |
| New AI-Powered Wi-Fi Biometrics WhoFi Tracks Humans Behind Walls with 95.5% Accuracy | <https://cybersecuritynews.com/new-ai-powered-wi-fi-biometrics-whofi-tracks-humans/>  |
| Chinese Hackers Attacking Windows Systems in Targeted Campaign to Deploy Ghost RAT and PhantomNet Malwares | <https://cybersecuritynews.com/chinese-hackers-attacking-windows-systems-in-targeted-campaign/>  |
| Google Launches OSS Rebuild to Strengthen Security of The Open-Source Package Ecosystems | <https://cybersecuritynews.com/google-launches-oss-rebuild-to-strengthen-security/>  |
| Stealthy Backdoor in WordPress Plugins Gives Attackers Persistent Access to Websites | <https://cybersecuritynews.com/stealthy-backdoor-in-wordpress-plugins/>  |
| New ACRStealer Abuses Google Docs and Steam for C2 Server Via DDR Technique | <https://cybersecuritynews.com/new-acrstealer-abuses-google-docs/>  |
| Operation CargoTalon Attacking Russian Aerospace & Defense to Deploy EAGLET Implant | <https://cybersecuritynews.com/operation-cargotalon-attacking-russian-aerospace/>  |
| Threat Actor Mimo Attacking Magento CMS to Steal Card Details and Bandwidth Monetization | <https://cybersecuritynews.com/threat-actor-mimo-attacking-magento-cms/>  |
| Weaponized LNK File Disguised as Credit Card Security Email Steals User Data | <https://cybersecuritynews.com/weaponized-lnk-file/>  |
| Lumma Stealer Via Fake Cracked Software Steals Login Credentials and Private Files | <https://cybersecuritynews.com/lumma-stealer-via-fake-cracked-software/>  |
| Silicon Valley Engineer Pleads Guilty to Stealing Missile Detection Data for China | <https://cybersecuritynews.com/silicon-valley-engineer-pleads-guilty/>  |
| Coyote Malware Abuses Microsoft’s UI Automation in Wild to Exfiltrate Login Credentials | <https://cybersecuritynews.com/coyote-malware-abuses-microsofts-ui-automation/>  |
| Researchers Unmasked Russia’s Most Secretive FSB’s Spy Network | <https://cybersecuritynews.com/russias-most-secretive-fsbs-spy-network/>  |
| Scavenger Malware Hijacks Popular npm Packages to Attack Developers | <https://cybersecuritynews.com/scavenger-malware-hijacks-popular-npm-packages/>  |
| Threat Actors Attacking Linux SSH Servers to Deploy SVF Botnet | <https://cybersecuritynews.com/threat-actors-attacking-linux-ssh-servers/>  |
| New Web3 Phishing Attack Leverages Fake AI Platforms to Steal Usernames and Passwords | <https://cybersecuritynews.com/new-web3-phishing-attack-leverages-fake-ai-platforms/>  |
| New ClickFake Interview Attack Using ClickFix Technique to Deliver GolangGhost Malware | <https://cybersecuritynews.com/new-clickfake-interview-attack-using-clickfix-technique/>  |
| Dark Web Travel Agencies Offering Cheap Travel Deals to Steal Credit Card Data | <https://cybersecuritynews.com/dark-web-travel-agencies-offering-cheap-travel-deals/>  |
| Exclusive! Threat Intelligence That Powers Best SOCs Worldwide Is Now Free  | <https://cybersecuritynews.com/free-threat-intelligence/>  |
| Iran’s Cyber Actors Attacking Global Airlines to Exfiltrate Sensitive Data | <https://cybersecuritynews.com/irans-cyber-actors-attacking-global-airlines/>  |
| Threat Actors Combine Android Malware With Click Fraud Apps to Steal Login Credentials | <https://cybersecuritynews.com/threat-actors-combine-android-malware-with-click-fraud-apps/>  |
| GLOBAL GROUP’s Golang Ransomware Attacks Windows, Linux, and macOS Environments | <https://cybersecuritynews.com/global-groups-golang-ransomware/>  |
| Greedy Sponge Hackers Attacking Financial Institutions With Modified Version of AllaKore RAT | <https://cybersecuritynews.com/greedy-sponge-hackers-attacking-financial-institutions/>  |
| DeerStealer Malware Delivered Via Weaponized .LNK Using LOLBin Tools | <https://cybersecuritynews.com/deerstealer-malware-delivered/>  |
| Threat Actors Hijack Popular npm Packages to Steal The Project Maintainers’ npm Tokens | <https://cybersecuritynews.com/threat-actors-hijack-popular-npm-packages/>  |
| Developers Beware of npm Phishing Email That Steal Your Login Credentials | <https://cybersecuritynews.com/developers-beware-of-npm-phishing-email/>  |

## Guides / Tools

|  |  |
| --- | --- |
| Σύντομη περιγραφή / Τίτλος | URL |
|  |  |

# References

1. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), <https://nvd.nist.gov/vuln-metrics/cvss>
2. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.
3. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

# Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

|  |  |
| --- | --- |
| **Vendor name / Platform** | **URL** |
| Wordpress | Wordfence Intelligence Vulnerability Database API <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/>Scan your WordPress website, <https://wpscan.com/scan/>  |
| Oracle | Critical Patch Updates, Security Alerts and Bulletins, <https://www.oracle.com/security-alerts/>  |
| Fortinet | Fortinet products, <https://www.fortiguard.com/psirt>  |
| IBM | Security bulletins, <https://cloud.ibm.com/status/security> Research, Collaborate and Act on threat intelligence, <https://exchange.xforce.ibmcloud.com/>  |
| MS Windows | The Microsoft Security Response Center (MSRC), <https://msrc.microsoft.com/update-guide/> |
| SAP | SAP Security Notes, <https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html>  |
| Dell | Security Advisories, Notices and Resources, <https://www.dell.com/support/security/en-us>  |
| HPE | HPE Security Bulletin Library, <https://support.hpe.com/connect/s/securitybulletinlibrary> Security Bulletins, <https://support.hp.com/us-en/security-bulletins>  |
| Cisco | Cisco Security Advisories, <https://sec.cloudapps.cisco.com/security/center/publicationListing.x>  |
| Palo Alto | Palo Alto Networks Security Advisories, <https://security.paloaltonetworks.com/>  |
| Ivanti | Security Advisory, <https://www.ivanti.com/blog/topics/security-advisory>  |
| Mozilla | Mozilla Foundation Security Advisories, <https://www.mozilla.org/en-US/security/advisories/>  |
| Android | Android Security Bulletins, <https://source.android.com/docs/security/bulletin/asb-overview>  |
| Zyxel | Security Advisories, <https://www.zyxel.com/global/en/support/security-advisories>  |
| D-Link | Global Security Advisories, Responses, and Notices, <https://supportannouncement.us.dlink.com/>  |
| Adobe | Security Bulletins and Advisories, <https://helpx.adobe.com/security/security-bulletin.html>  |
| Siemens | Siemens ProductCERT and Siemens CERT, <https://www.siemens.com/global/en/products/services/cert.html>  |
| Splunk | Splunk Security Advisories, <https://advisory.splunk.com/>  |